OASIS ebXML Registry Security Sub Team

Security Proposal for ebXML Registry V2

Oct 1, 2001

V 0.2

Authors:

Suresh Damodaran
Sanjay Patil

Contributors:

Farrukh Najmi
Sekhar Vajjhala

Status of this Document

This document contains a proposal for security specifications for the upcoming Version 2 release of ebXML Registry (“registry”). This is still a work in progress.

Revision History

Date	Version	Who	What
8/13/2001	V 0.10	SD	First version
8/20/2001	V 0.11	SD	Added Sec 1.1 per comments by Farrukh. Did some editorial changes.
8/27/2001	V 0.12	SD	Expanded Sec 3 per Sanjay’s comments. Removed Sec 4. Expanded issues.
8/28/2001	V 0.13	SP	Entered “Type category” info in Table 2 as per discussions
9/06/2001	V 0.14	SD	Made minor edits – added Type F
09/19/01	V 0.15	SD	Included Sanjay’s use cases
10/01/01	V 0.2	SD	Updated actors, edited use cases section to conform.

1 Overview

The goal of this paper is to evaluate the security concerns for V1, identify the absolutely required features for V2, and propose a means to implement these features. We outline some of the concerns of registry users and use cases. The list of deliverables are at the end.

1.1 Security Related Issues with V1

The broad issues related to security in version 1 of ebXML Registry are the following.

1. There is a lack of specificity on how to apply security standards. E.g., Digital Signature.
2. Some of the security risks are addressed but are costly or difficult to implement. E.g., Digital Signature for authentication of all Registry Users may not be necessary for some Registry Users such as Registry Guest.
3. Some security risks are not addressed in this specification at all. E.g., Security Policy maintenance.
4. Version 1 needs to be aligned with other security related OASIS TCs and/or other relevant standards. E.g., XACML

The major goal of this paper is to identify the absolutely necessary features for V2 and suggest a proposal for providing those features.

1.2 Glossary

This document uses terminology in RFC 2828 for all terms related to security.

2 Registry Users

We describe the actors who use the registry from the point of view of security and analyze the security concerns of the registry below. This analysis leads up to the security requirements for V2. Some of the actors are defined in Section 9.4.1 of [ebRS]. Note that same entity may take on multiple roles. For example, a Registry Operator and Registry Administrator may have the same identity.

Actor	Function	ISO/IEC 11179	Comments
Registry Operator	Hosts the RegistryObjects	Registration Authority (RO)	
Registry Administrator	Evaluates and enforces registry security policy. Facilitates definition of the registry security policy.		MAY be the same as Registry Operator
Registered User	Has a *contract* with the Registry Operator and MUST be authenticated by Registry Operator.		The contract could be a ebXML CPA conforming or some other form of contract. Section 6.1 [ebRS].
Registry Guest	Has no *contract* with Registry Operator. Does not have to be authenticated for Registry access. Cannot change contents of the Registry (MAY be permitted to *read* some RegistryObjects.)		Note that a Registry Guest is *not* a Registry Reader.
Registry Publisher	A Registered User who does lifecycle operations on	Submitting Organization (SO)	

	permitted RegistryObjects.		
Registry Reader	A Registered User who has only *read* access		
Registry Content Owner	Creates Registry Objects	Responsible Organization (RO)	RO MAY have the same identity as SO
Registry Client	Registered User or Registered Guest		

Note:

1. In V2, we are not distinguishing between Registry Submitter/Registry Publisher and Registry Content Owner.
2. Registration of a user happens out-of-band for V2.
3. For V2 we do not distinguish between Registry Administrator and Registry Operator.

3 Security Concerns

The security risks broadly stem from the following concerns. We analyze these concerns to understand how these are addressed in the current specs and how these needs to be addressed in V2 of the specs.

1. Is the content of the registry (data) trustworthy?

    a) How to make sure "what is in the registry" is "what is put there" by a registry publisher? This concern can be addressed by ensuring that the publisher is authenticated using digital signature (Source Integrity), message is not corrupted during transfer using digital signature (Data Integrity), and the data is not altered by unauthorized subjects based on access control policy (Authorization)

    b) How to protect data while in transmission? What are the most critical types of data?

Communication integrity has two ingredients – Data Integrity (addressed in 1a) and Data Confidentiality that can be addressed by encrypting the data in transmission. Replay attack.

c) Is the content up to date? The versioning as well as any time stamp processing, when done securely will ensure the "latest content" is guaranteed to be the latest content. Authorization with access control policy could solve this problem.

d) How to ensure only bona fide publishers add contents to registry? Ensuring Source Integrity (as in 1a).

e) How to ensure that bona fide publishers add contents to registry only at authorized locations? (System Integrity

f) What if the publishers deny modifying certain content after-the-fact? To prevent this (Nonrepudiation) audit trails are to be kept which contain signed message digests.

g) What if the reader denies getting information from the registry?

h) How to ensure integrity of classification schemes as well as dynamic data (classification & association) (Correctness Integrity, may not be a security issue)

2. How to provide selective access to registry content? The broad answer is, by using an access control policy – applies to (a), (b), and (c) directly.
    a) How does a registry publisher restrict access to the content to only specific registry readers?
    b) How can a registry publisher allow some "partners" (fellow publishers) to modify content?
    c) How to provide selective access to partners the registry usage data?
    d) How to prevent accidental access to data by unauthorized users? Especially with hw/sw failure of the registry security components? The solution to this problem is by having System Integrity.
    e) Data confidentiality of RegistryObject
3. How do we make "who can see what" policy itself visible to limited parties, even excluding the administrator (self & confidential maintenance of access control policy). By making sure there is an access control policy for accessing the policies themselves.

4. How to transfer credentials? The broad solution is to use credentials assertion (such as being worked on in SAML)
   a) How to transfer credentials (authorization/authentication) to federated registries?
   b) How do aggregators get credentials (authorization/authentication) transferred to them?
   c) How to store credentials through a session?
   d) How to store and use credentials for queries triggered by a single query? – Implementation specific – becomes 4a when multiple registries.
5. How to bind the registry security mechanisms to security infrastructure? The definition of the security infrastructure and binding to the infrastructure to do security related processing will solve this problem.

4 Use Cases

The use cases below combine the actors defined earlier with the actions (defined below) with the security concerns described earlier.

4.1 Actions

Publish Actions ("Life Cycle Actions[sd1]" as in Section 6.4.3 and 7.1 [ebRS])
submitObject[sd2]
approveObject
deprecateObject
removeObject
Read Actions
Query, audit query
Update Actions
update (same as submitObject above)[sd3]
Administrative Actions
Retrieve operational statistics, shutdown, startup

4.2 Use cases

1. Registry Operator wants to differentiate between Registered Users and Registry Guests.
   Business use case example – Registry Operator wants to provide access to richer capabilities to Registered users and limited capabilities to Registry Guests.
2. Registry Operator wants to decide whether or not to allow an action that Registry Client wants to perform
   Business use case example – allow only Registered Users to "Publish"
3. Registry Operator wants to restrict execution of administrative processes to only Registry Administrator
   Business use case example – prevent shut down of the Registry by users other than Registry Administrator
4. Registry Operator wants to restrict operations on Registry to only authenticated and authorized Registry Clients
   Business use case example – prevent access to Registry by a user who is not Registered and impersonating as a Registered User
5. Registry Operator wants to restrict sending Response objects to autheticated and authorized Registry Clients
   Business use case example – prevent sending sensitive Response Object to unauthenticated and unauthorized recipients
6. Registry Client wants to ensure that the Registry Operator is authenticated
   Business use case example – Registry client does not want to publish his sensitive business content to a hoax Registry
7. Registry Client wants to restrict, which other Registry Clients can access the Registry Content it is publishing to the Registry.

8. Registry Client wants to ensure that the Registry Content it is publishing to Registry is not visible on the network
   Business use case example – Credit Card Information
9. Registry Client wants to ensure that the Registry Content it is publishing to Registry is not changed on the network
10. Registry Client wants to ensure that the Registry Content it has published to Registry is not visible to the Registry Administrator
11. Registry Client wants to ensure that the Registry Content it has published to Registry is not changed by the Registry Administrator
12. Registry Client wants to ensure that the Registry Content sent to it by Registry is not visible on the network
13. Registry Client wants to ensure that the Registry Content sent to it by Registry is not changed on the network
14. Registry Client wants to ensure that the source of Registry Content received from Registry is verifiable
    Business use case example – The information claiming to have been published by a company XYZ was really published by the company XYZ.
15. Registry Client wants to build and store sufficient evidence of its requests being received by Registry
16. Registry Client wants to build and store sufficient evidence of response being received from Registry
17. Registry wants to build and store sufficient evidence of response being sent to Registry Client
18. Registry wants to build and store sufficient evidence of receiving request from Registry Client
19. Registry Client wants to retrieve information about the access of a particular Registry Object
    a. by all or a specified set of Registry Clients,
    b. since the creation of the Registry Object,
    c. from a specified time,
    d. from a specified identifiable Registry event.

4.2.1 Relationship to Security Risks

Classification of use cases in terms of security concerns

Error! Reference source not found. – Role Identification (Risk 2)

Error! Reference source not found.,**Error! Reference source not found.**, **Error! Reference source not found.**,**Error! Reference source not found.**- Access Control (Risk 2)

Error! Reference source not found.,**Error! Reference source not found.** – Peer Entity Authentication (Risk 1)

Error! Reference source not found. – Data Confidentiality (in persistence) (Risk 2e)

Error! Reference source not found.– Data Integrity (in persistence) (Risk 1)

Error! Reference source not found.,**Error! Reference source not found.**– Data Confidentiality (in transit) (Risk 1)

Error! Reference source not found.,**Error! Reference source not found.**– Data Integrity (in transit) (Risk 1)

Error! Reference source not found. – Data Origin Authentication (Risk 1)

Error! Reference source not found.,**Error! Reference source not found.**,**Error! Reference source not found.**,**Error! Reference source not found.** – NonRepudiation (Risk 1f, 1g)

Error! Reference source not found. – Auditing (Risk 2c)

5 Addressing the Risks

5.1 Risk Management in Current Specs

Section 9 of [ebRS] describes the current techniques to address the risks outline earlier. We briefly outline the current techniques and which risks they manage.

5.1.1 Current Techniques

Refer to the table in Section 3.
NA – Not Available

Concern	Techniques	Issues
1a: How to make sure “what is in the registry” is “what is put there” by a registry publisher?	1. Message Payload Signature [Sec 9.1.1]	2. Costly to process and maintain. Instead: (a) signature for packages? (b) Signature for envelopes only, and signature discarded 2. Not clear on the definition of “contents”
1b: How to protect data while in transmission? What are the most critical types of data?	1. Message Payload Signature [Sec 9.1.1]	1. Same as 1a. above. 2. Confidentiality requires encryption of transmitted data
1c: Is the content up to date?	NA	1. Versioning not included in signing
1d: How to ensure only bona fide publishers add contents to registry?	1. Digital signature and trust management based authentication	
1e: How to ensure that bona fide publishers add contents to registry only at authorized locations?	NA	
1f: What if the publishers deny modifying certain content after-the-fact?	1. Only the publisher can modify the content	
1g: How to ensure integrity of classification schemes as well as dynamic data (classification & association)	NA	
2a: How does a registry publisher restrict access to the content to only specific registry readers?	1. An access control policy	1. Only default access control policy that allows authenticated Registry Clients unlimited access to the content 2. RS did not have interfaces to manipulate access control policy 3. Current granularity of access control is at the method level – better if

		we can restrict the methods to create/update/version/delete
2b: How can a registry publisher allow some “partners” (fellow publishers) to modify content?	1. An access control policy	1. Same as 2a
2c: How to provide selective access to partners the registry usage data?	NA	
2d: How to prevent accidental access to unsolicited data? Especially with hw/sw failure of the registry security components?	NA	
2e: Data Confidentiality of Registry Content while in storage	NA – recommends encryption	
3: How do we make “who can see what” policy itself visible to limited parties, even excluding the administrator (self & confidential maintenance of access control policy)	NA	
4a: How to transfer credentials (authorization/authentication) to federated registries?	NA	
4b: How do aggregators get credentials (authorization/authentication) transferred to them?	NA	
4c: How to store credentials through a session?		1. No session concept at this time- so not an issue
4d: How to store and use credentials for queries triggered by a single query?	NA	
5: How to bind the registry security mechanisms to security infrastructure?	1. Trust management services are mentioned	1. No clear guidelines on how to use the services

5.2 Newer Version of Security

We describe below how the newer version of security would address the same security concerns discussed earlier. We need to prioritize which of the risks to be addressed for the next version. Below is the table that outlines the prioritized list.

Legend:

Type in the table enumerates as follows:

Type A) Absolutely required for V2. Belongs to “bug fix” category to V1

Type B) Absolutely required for V2. New for V2, not considered for V1.

Type C) Having this feature will give V2 Competitive advantage. Neither Type A or Type B.
Type D) Nice to have in V2 – will make V2 really convenient to use and rich.
Type F) Futuristic

Concern	Techniques	Issues	Type
1a: How to make sure "what is in the registry" is "what is put there" by a registry publisher?			C
1b: How to protect data while in transmission? What are the most critical types of data?			C
1c: Is the content up to date?			D
1d: How to ensure only bona fide publishers add contents to registry?			A
1e: How to ensure that bona fide publishers add contents to registry only at authorized locations?			F
1f: What if the publishers deny modifying certain content after-the-fact?			C
1g: How to ensure integrity of classification schemes as well as dynamic data (classification & association)			Out of scope
1h: What if the reader denies getting information from the registry?			C
2a: How does a registry publisher restrict access to the content to only specific registry readers?			A
2b: How can a registry publisher allow some "partners" (fellow publishers) to modify content?			A
2c: How to provide selective access to partners the registry usage data?			D
2d: How to prevent accidental access to unsolicited data? Especially with hw/sw failure of the registry security components?			F
2e: Data Confidentiality of Registry Content while in			C

repository			
3: How do we make “who can see what” policy itself visible to limited parties, even excluding the administrator (self & confidential maintenance of access control policy)			F
4a: How to transfer credentials (authorization/authentication) to federated registries?			F
4b: How do aggregators get credentials (authorization/authentication) transferred to them?			C
4c: How to store credentials through a session?			F
4d: How to store and use credentials for queries triggered by a single query?			Implementation Detail
5: How to bind the registry security mechanisms to security infrastructure?			D

6 Deliverables

The deliverables for V2 are:

1. This document, i.e., security proposal
2. A separate document to address 1d above, with primary focus on Data Integrity

We did not address 2a and 2b through authorization policy schema and cookie cutter policies for V2, though we are currently working on it, and we plan to address these going forward.

7 Issues

1. Reconcile the actors in the registry to actors in this doc. ISO 11179 terminology also needs to be reconciled.
2. Registry Profiles need to be defined. Currently, there is no clear definition of the Registry profile.
3. Bootstrapping process needs to be defined.
4. Update operation currently is done through submitObjects(). Does a new version get assigned to the RegistryObject when a submitObject() is done?
5. The steps involved in executing the relevant use cases from the point of view of security needs to be described.

8 References

[ebRS] ebXML Registry Services Specification

http://www.ebxml.org/specs/ebRS.pdf

[ebRIM] ebXML Registry Information Model 1.0

http://www.ebxml.org/specs/ebRIM.pdf

[ISO1] ISO/IEC 11179-1 Specification and standardization of data elements – Part 1
http://www.sdct.itl.nist.gov/~ftp/l8/11179/11179-1.htm

[UUID] DCE 128 bit Universal Unique Identifier
http://www.opengroup.org/onlinepubs/009629399/apdxa.htm#tagcjh_20

http://www.opengroup.org/publications/catalog/c706.htmttp://www.w3.org/TR/REC-xml

Page: 4
[sd1]Could not find these on the RegistryObject – found only on client requests
Page: 4
[sd2]See Issue 1
Page: 4
[sd3]The idea is to change the version number when you submit a new version?